UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/700,656	02/14/2001	Harald Vater	JEK/VATER	7577

7590 07/20/2006

Bacon & Thomas
Fourth Floor
625 Slaters Lane
Alexandria, VA 22314-1176

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 07/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/700,656	VATER ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) *1-25,34-41 and 43* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *26-33 and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 08 May 2006. By this response, Claims 28, 30, and 33 have been amended. No claims have been added or canceled. Claims 1-25, 34-41, and 43 were previously withdrawn from further consideration as being directed to nonelected inventions. Claims 26-33 and 42 are currently under consideration in the present application.

Response to Amendment

2. The Examiner notes that the present response fails to comply with the provisions of 37 CFR 1.121. Specifically, Claims 1-25, 34-41, and 43 are listed with the status identifier "Previously Presented"; however, the claims were withdrawn from further consideration and should therefore be labeled with the status identifier "Withdrawn". See 37 CFR 1.121(c). In the interest of advancing the prosecution of the present application, the amendment has been considered as though it were in compliance with 37 CFR 1.121; however, Applicant is reminded that future responses must comply with the provisions set forth in 37 CFR 1.121.

Election/Restrictions

3. Applicant argues that the election in the response received 16 November 2005 was wrongly characterized as without traverse in the previous Office action. Specifically, Applicant further argues that one of the criteria for a proper requirement for restriction is that there be a burden on the Examiner if restriction were not required, and that Applicant argued in the response of 16 November 2005 that because the claims were already examined, there could not be a burden on the Examiner. However, the Examiner respectfully disagrees.

First, the Examiner notes that, as per MPEP § 811 and 37 CFR 1.142(a), although a requirement for restriction is "normally" made before any action on the merits, it may be made at any time before final action. Further, as the present application was filed under 35 U.S.C. 371, unity of invention practice is applicable, and as per 37 CFR 1.499, the requirement to elect an invention "may be made at any time before the final action **at the discretion of the examiner**" (emphasis added). See also MPEP § 1893.03(d). As the application was subject to a request for continued examination under 37 CFR 1.114, it is considered to have been before final action at the time the requirement was made.

Further, the Examiner notes that, in the requirement for restriction mailed 17 October 2005, the Examiner set forth specific reasons why further examination of the claims would place undue burden on the Examiner, namely that Applicant's arguments in the response received 22 July 2005 being directed to substantially divergent

limitations in the different groups of claims, combined with the presence of distinct inventions which do not share a single general inventive concept as set forth in the restriction requirement, suggested that **further** examination of the distinct groups would require substantially divergent searches and therefore that further prosecution of the differing groups would be divergent. This divergent further examination was considered to place an undue burden on the Examiner, and thus the requirement for restriction was made. The Examiner further notes that Applicant's arguments in the election received 16 November 2005 **did not address the specific reasons that the Examiner provided** as to why the requirement for restriction was proper, such reasons being noted above, and instead amounted to a mere allegation that the requirement for restriction was improper.

Finally, the Examiner notes that, because unity of invention practice, and not restriction practice, is applicable because the application was filed as a national stage application under 35 U.S.C. 371, the factors listed in MPEP § 803 noted by the Applicant at page 10 of the present response, namely that the inventions must be independent or distinct and there would be a serious burden on the Examiner if restriction was not required, are not the criteria for a restriction under unity of invention practice. Rather, the requirement for the Examiner is to list the groups of inventions and show that each group lacks unity with each other group specifically describing the unique special technical feature of each group, following the principles of unity of invention. See MPEP §§ 823, 1893.03(d), and 1850. The Examiner provided such a

list and showing of lack of unity in the requirement mailed 17 October 2005, and Applicant's traversal did not include a rebuttal of such showing of lack of unity.

4. In summary, the Examiner again acknowledges Applicant's election of Group II, Claims 26-33 and 42 in the reply filed on 16 November 2005. Because applicant did not distinctly and specifically point out the supposed errors in the restriction requirement, the election has been treated as an election without traverse (MPEP § 818.03(a)).

Response to Arguments

5. Applicant's arguments filed 08 May 2006 have been fully considered but they are not persuasive.

Applicant traverses the rejections of Claims 26-32 and 42 under 35 U.S.C. 102(e) as anticipated by Jakobsson, US Patent 6049613, and of Claim 33 under 35 U.S.C. 103(a) as unpatentable over Jakobsson. Specifically, Applicant argues that "the Jakobsson patent fails to disclose or suggest a data carrier, as claimed, in which operating program commands are arranged to prevent signals caused by execution of the commands from being used to infer data being processed" (see page 11 of the present response). However, none of the above claims under consideration (i.e. Claims 26-33 and 42) recites the data carrier or operating commands as asserted by Applicant, and therefore it is immaterial whether Jakobsson discloses, teaches, or suggests such limitations.

Applicant further argues that Jakobsson is concerned with data protection but is not concerned with data inference by interception of emissions occurring during data protection, whereas the present invention "applies to the situation where signal emissions are vulnerable to interception" (see page 12 of the present response). However, the Examiner notes that Claim 26 explicitly recites "A method for protecting secret data" and neither Claim 26 nor its dependents recites anything regarding interception of signal emissions.

Applicant also argues that Jakobsson is not concerned with the recited limitations of Claim 1 (see page 12 of the present response); however, the Examiner notes that Claim 1 was withdrawn from further consideration.

Applicant additionally quotes from the previous Office action and alleges that "**The Examiner has based the rejection on features that are not even claimed, while ignoring what is actually claimed, namely arranging operating program commands in such a way that the data is not detectable from outside the chip**" (pages 12-13 of the present response, emphasis in original). However, the Examiner respectfully disagrees with this allegation, noting that Claim 26 **is, in fact, directed to protecting data** by a method including "falsifying input data", as noted in the previous Office action. The Examiner further notes that Claim 26 makes **no mention whatsoever** of arranging operating program commands. Applicant further argues that the Examiner has "ignored a number of specific claim limitations" which are listed at pages 13-14 of the present response. However, the Examiner again notes that there is **no recitation whatsoever** in Claim 26 or its dependents of "**operating program**

commands that cause signal emissions detectable outside a chip" or "selection or execution of the **operating program commands** in such as [sic] way that '***the operating program commands cannot be inferred from said signals that are caused by execution of said commands and that have been detected outside the semiconductor chip***'" (pages 13-14 of the present response, emphasis in original). Because these **limitations do not appear in the claims under consideration** (i.e. Claims 26-33 and 42), the allegation that these limitations were ignored in making the rejections of the claims under consideration is entirely spurious.

In summary, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 112

6. The rejection of Claims 28-30 and 33 under 35 U.S.C. 112, second paragraph, is withdrawn in light of the amendments to the claims. The rejection of Claim 42 under 35 U.S.C. 112, second paragraph, is maintained as set forth below, as the present

response does not appear to address the rejection, although it is acknowledged (see page 11 of the present response).

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 42 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 42 recites the limitation "the security-relevant operations". There is insufficient antecedent basis for this limitation in the claims, although it appears to refer to the "one or more operations" of Claim 26.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 26-32 and 42 are rejected under 35 U.S.C. 102(e) as being anticipated by Jakobsson, US Patent 6049613.

In reference to Claim 26, Jakobsson discloses a method of protecting secret data, where the method includes falsifying input data by combination with auxiliary data (column 5, line 56-column 6, line 42; column 6, line 56-column 7, line 3), and combining the output data with an auxiliary function value in order to compensate for the falsification of the input data, where the auxiliary value was previously determined (column 7, lines 48-65; column 10, lines 5-6).

In reference to Claim 27, Jakobsson further discloses that the combination with the auxiliary function value is performed before execution of a non-linear operation (column 7, lines 48-65, where this is performed before execution of the operation at column 7, 66-column 8, line 28).

In reference to Claim 28, Jakobsson further discloses that the auxiliary data are varied (column 6, lines 33-42, where different keys are used).

In reference to Claims 29-32, Jakobsson further discloses that new auxiliary values can be generated by combining existing values, that auxiliary data are selected randomly, pairs of auxiliary data and auxiliary function values are generated, and the auxiliary data are random numbers (column 6, lines 33-42; column 7, lines 18-21, where keys are randomly chosen).

In reference to Claim 42, Jakobsson further discloses that operations include permutations of data (see column 6, lines 50-55; column 7, lines 29-33).

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jakobsson.

Jakobsson discloses everything as applied to Claim 26. Jakobsson further discloses various encryption methods (column 6, lines 11-42; column 1, lines 19-50); however, Jakobsson does not explicitly disclose combining data using an XOR operation. Official notice is taken that it is well known in the art to use XOR for an easily executed encryption operation combining data with a key. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use XOR for the combination operation in order to take advantage of the simplicity of the operation.

Conclusion

13. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100